Мониторинг в режиме “promiscuous” в сетях Ethernet и Wi-Fi

Аннотация

В данной статье рассматриваются вопросы, связанные с использованием программных средств для мониторинга проводных и беспроводных сетей. В статье показаны способы достижения прозрачности сети в различных сетевых конфигурациях, подробно разъяснены основные принципы сетевого мониторинга и описаны решения типовых проблем при работе с программами сетевого мониторинга.

Содержание

Что такое мониторинг в режиме "promiscuous"

В компьютерных сетях режим *promiscuous* - это особый режим оборудования Ethernet, как правило сетевых интерфейсных карт (NIC), который позволяет карте получать весь трафик сети, даже если этот трафик не адресован конкретно данной карте. По умолчанию NIC игнорирует весь не адресованный ему трафик путем сравнения адреса назначения Ethernet-пакета и аппаратного адреса принимающего устройства (MAC-адреса). Хотя такая схема работы вполне оправдана технически, режим не-*promiscuous* существенно затрудняет работу программ сетевого анализа и мониторинга, применяемых для диагностики сетевых проблем и учета трафика.

В более широком смысле режим *promiscuous* также означает прозрачность сети с определенной точки наблюдения, но при этом не подразумевается обязательного перевода адаптеров в такой режим. В современном оборудовании и программном обеспечении часто реализованы и другие способы мониторинга для достижения полной видимости всех сетевых процессов. В данной статье мы обсудим различные способы обеспечения прозрачности проводных и беспроводных сетей в различных конфигурациях и с разными наборами сетевого оборудования.

Применение на практике

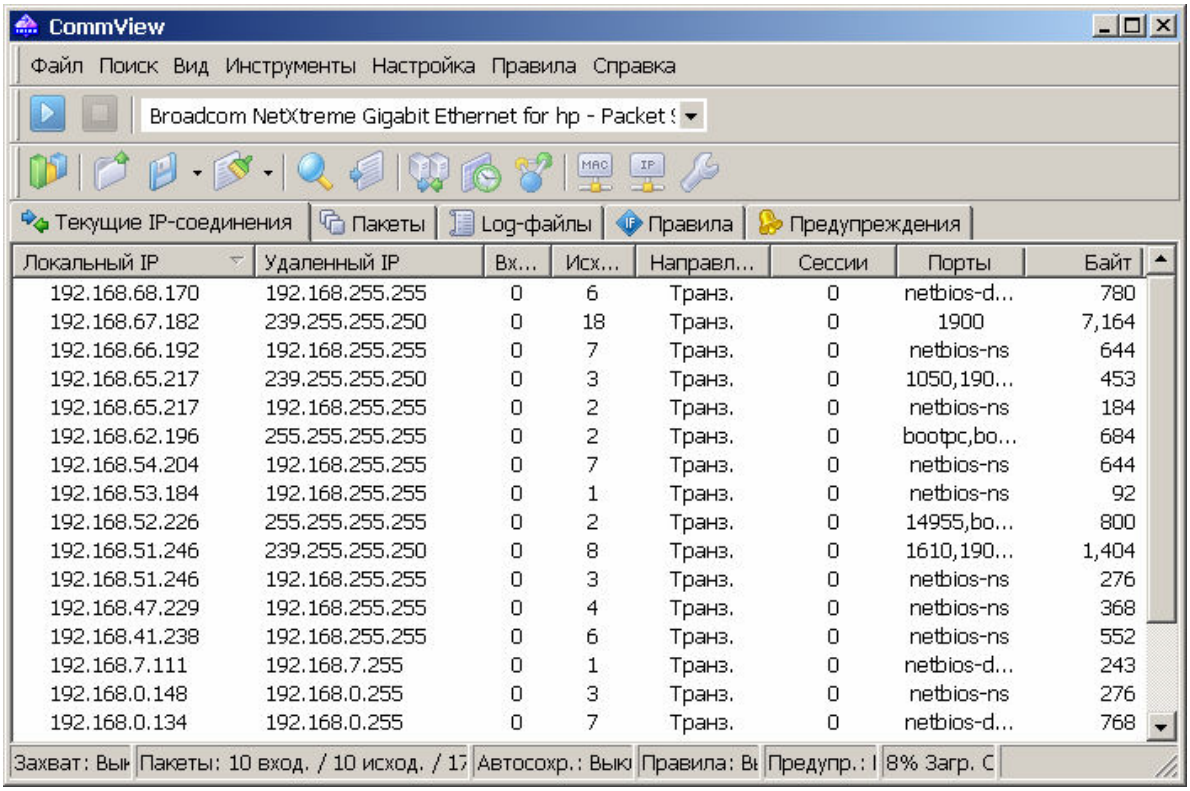
Так зачем же может потребоваться мониторинг сети вне нашего собственного компьютера? Вот простая ситуация: ваша сеть состоит из трех компьютеров A, B и C, на компьютере A запущен сетевой анализатор, и вы можете наблюдать не только входящий/исходящий трафик на компьютере A, но и данные, проходящие между компьютерами B и C. Это нужно при работе с сетевыми анализаторами, системами учета трафика и мониторинга сетевого контента. В принципе, вы можете запустить эти программы на каждом компьютере, но это довольно неудобно, поскольку у вас перед глазами не будет всей полноты картины.

Целями данной статьи являются ответы на часто задаваемые вопросы по работе с программами компании TamoSoft: CommView (сетевой анализатор для проводных сетей), CommView for WiFi (сетевой анализатор для беспроводных сетей), CommTraffic (система учета трафика) и NetResident (система мониторинга сетевого контента). Принципы мониторинга и топологии сетей, которые будут обсуждаться в дальнейшем, носят общий характер, поэтому могут быть применены к любым другим программам мониторинга/анализа сетей Ethernet и Wi-Fi, независимо от производителя и операционной системы.

Сети Ethernet, хабы и коммутаторы

В сетях Ethernet хабы (концентратор, hub) и коммутаторы (switch) являются центральными точками подключения к сети компьютеров или других сетевых устройств. В совокупности эти компьютеры составляют сегмент сети. В рамках этого сегмента все компьютеры могут "общаться" непосредственно друг с другом. Хабы – менее "интеллектуальные" устройства, нежели коммутаторы: они просто принимают входящие пакеты через один порт и передают их на другие порты. Это их свойство отлично подходит для мониторинга в режиме *promiscuous.*

В отличие от хабов, коммутаторы анализируют все пакеты по мере их поступления и проверяют MAC-адреса источника и назначения. После этого пакет передается в нужный порт. В коммутируемых сетях сетевой анализатор ограничен в своих функциях приемом broadcast- и multicast-пакетов, а также приемом трафика, передаваемого и получаемого тем компьютером, на котором установлен анализатор. Ниже показана типичная картина сетевой активности в коммутируемой сети:

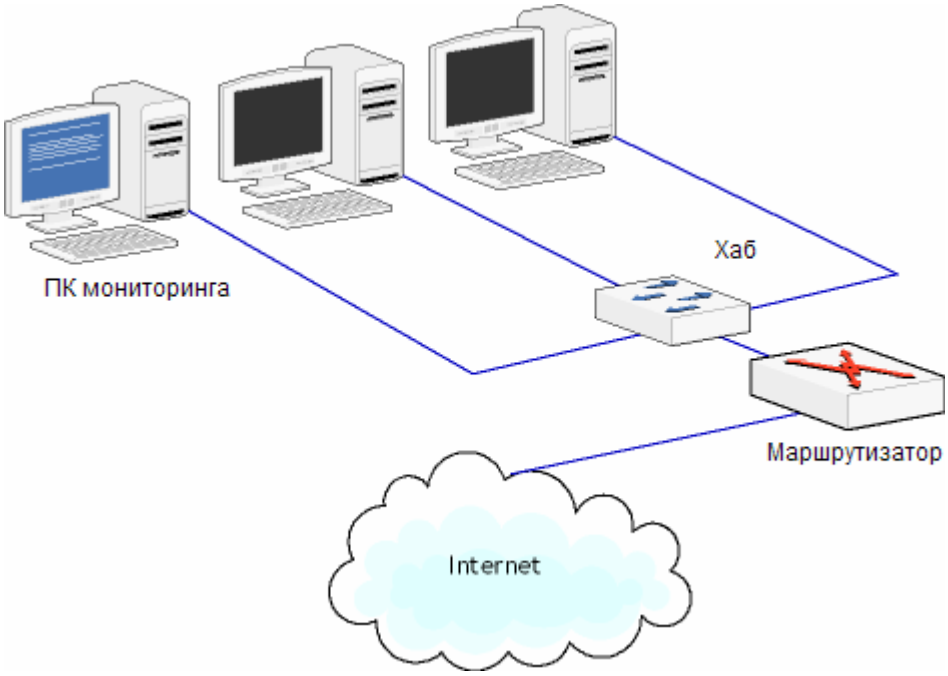


На иллюстрации можно увидеть большое количество broadcast-пакетов, посылаемых хостами локальной сети на IP-broadcast-адреса, при этом вы не можете увидеть нормальный unicast-трафик между этими хостами или между этими хостами и Интернетом. Несмотря на то, что большинство коммутаторов не позволяют осуществлять мониторинг в режиме promiscuous, многие коммутаторы могут быть сконфигурированы так, чтобы переправлять пакеты на специальный порт для мониторинга. Ниже мы обсудим применение хабов и коммутаторов в мониторинге сетей.

Мониторинг с помощью хабов

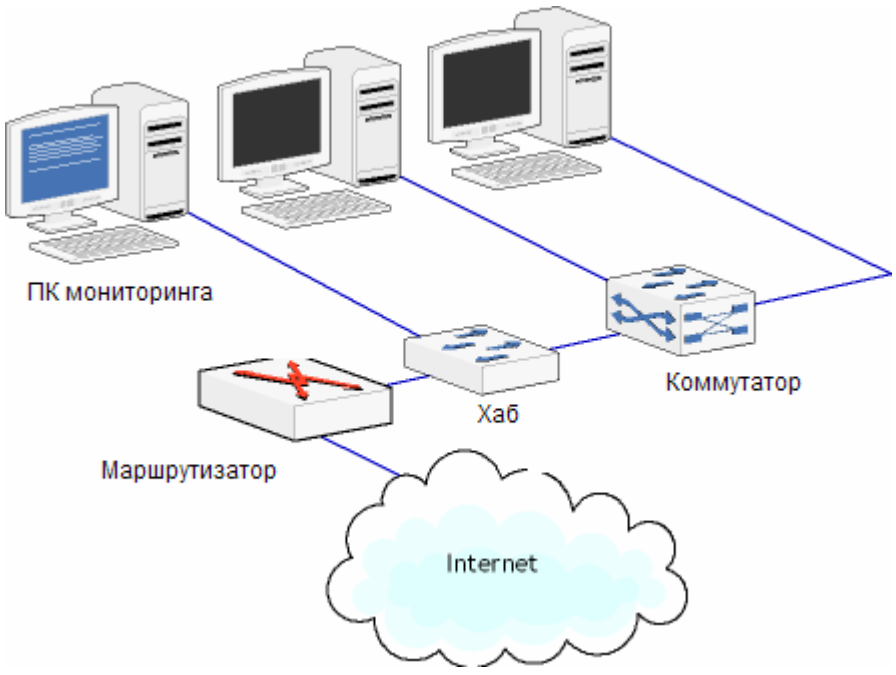
В небольших сетях хабы достаточно распространены из-за их небольшой стоимости, но все же следует обратить внимание на возможные проблемы в их применении. Во-первых, хабы открыты для несанкционированного мониторинга изнутри вашего сегмента сети, поскольку каждый порт может быть использован для promiscuous-мониторинга. Во-вторых, различные виды "интеллектуальных" хабов ("auto-sensing", "dual-speed", "switching", "intelligent") могут не позволить вам вести мониторинг всего сегмента сети. Эта проблема обсуждается в следующем разделе, а сейчас мы рассмотрим несколько вариантов сетей с использованием хабов.

Вариант 1



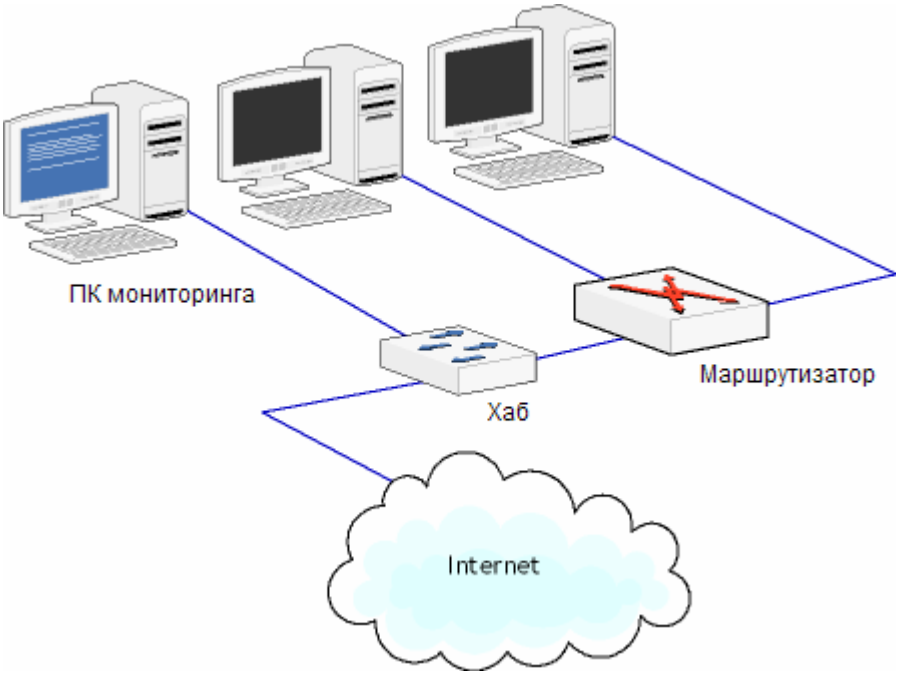
Это наиболее простой и очевидный вариант. Здесь любой компьютер, подключенный к хабу, может быть компьютером для мониторинга, поскольку хаб передает принятые/переданные данные от маршрутизатора (router) на все порты. Также отметим, что возможен мониторинг обмена между локальными ПК.

Вариант 2



В этом варианте хаб находится между маршрутизатором и коммутатором. Вы можете наблюдать данные, передаваемые/получаемые из Интернета, но данные, которыми обмениваются локальные ПК, вам недоступны.

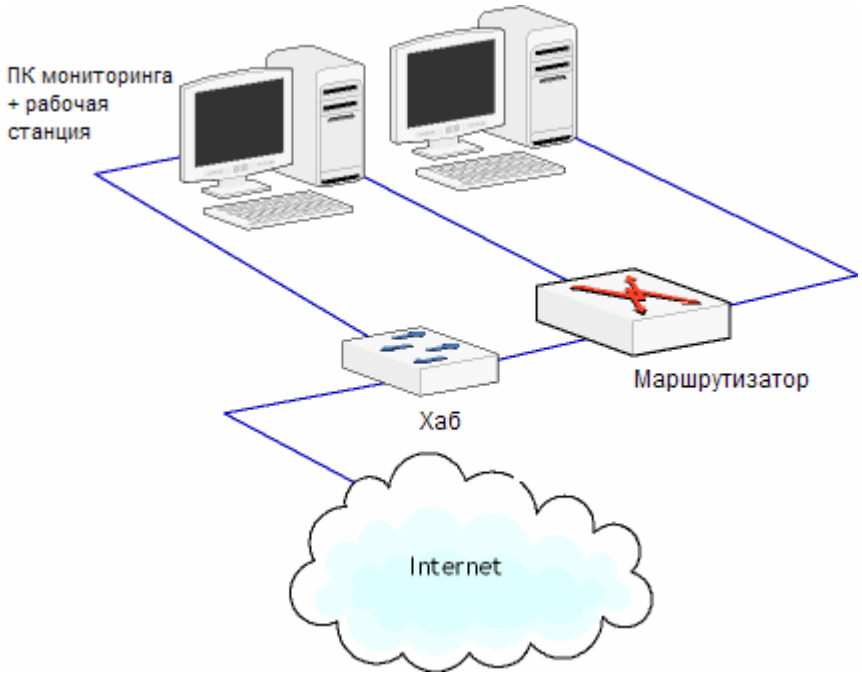
Вариант 3



В данном варианте показано, как можно осуществлять мониторинг небольшой локальной сети, в которой нет коммутатора. Это типичная топология домашней или небольшой офисной сети, где маршрутизатор совмещен с коммутатором, к которому в свою очередь подключены другие компьютеры. Для мониторинга данных, передаваемых или принимаемых из Интернета, вы можете установить хаб между Интернетом и вашим маршрутизатором. Важно отметить, что программа сетевого мониторинга не сможет различать трафик от разных рабочих станций, если у этих рабочих станций, находящихся за маршрутизатором, не будет внешних (routable) IP-адресов. Если у них нет внешних IP-адресов, то все пакеты будут иметь один IP-адрес, т.е. публичный IP-адрес вашей сети.

Компьютер для мониторинга, находящийся вне вашего сегмента сети, должен быть абсолютно пассивным, т. е. его сетевой интерфейс должен использоваться только для перехвата данных. Этого можно достичь путем назначения сетевой карте внутреннего (non-routable) IP-адреса, например, 10.0.0.1, или вообще отключив от адаптера TCP/IP-стек. Для достижения такой пассивности может быть использован кабель "только для чтения"; этот метод мы обсудим ниже.

Вариант 4



Этот вариант является разновидностью варианта №3, но здесь функции мониторинга выполняет одна из рабочих станций, имеющая две сетевых карты: первая используется для обычного обмена данными внутри локальной сети, а вторая – для мониторинга. Для приведения второй NIC в пассивное состояние следует выполнить действия, описанные для варианта №3. Этот вариант следует рассматривать как бюджетное решение.

Хабы: возможные проблемы

Помимо того, чтобы хабы имеют меньшую производительность, нежели коммутаторы, вы можете столкнуться еще с двумя проблемами при promiscuous-мониторинге с использованием хабов.

Первая проблема связана с двухскоростными ("auto-sensing") хабами, которые поддерживают аппаратуру, работающую как со скоростью 10 Мбит/с, так и 100 Мбит/с. Такие хабы не передают данных из портов, работающих со скоростью 10 Мбит/с, портам, работающим со скоростью 1000 Мбит/с и наоборот. Эту проблему можно решить, настроив все ваше оборудование на какую-то одну скорость. Большинство многоскоростных карт дают вам возможность задать желаемую скорость.

Вторая проблема связана с хабами, которые только формально называются хабами, но внутри являются коммутаторами (так делают некоторые производители, например, Linksys). Производители часто называют их "интеллектуальными" или "коммутируемыми", но могут и не делать это. Даже если в документации этого явно не указано, хаб вполне может оказаться коммутатором. Единственный способ выяснить это – попробовать поработать с такой аппаратурой. Старые и недорогие хабы чаще всего оказываются "настоящими" хабами. Другим хорошим индикатором того, что перед вами "настоящий" хаб – это индикатор (LED) коллизий. В коммутируемых сетях коллизий не бывает, поэтому у коммутатора вы такого индикатора не увидите.

Кабели "только для чтения"

Как упоминалось выше, работа в сети с хабом и мониторинг компьютера снаружи маршрутизатора может представлять угрозу для сетевой безопасности. Этой угрозы можно избежать, заставив компьютер работать только в режиме приема. Самым надежным решением будет использовать Ethernet-кабель только "для чтения". Такой кабель можно сделать с помощью щипцов из обычного кабеля CAT5 и двух разъемов RJ-45. Схема прокладки проводов показана ниже.

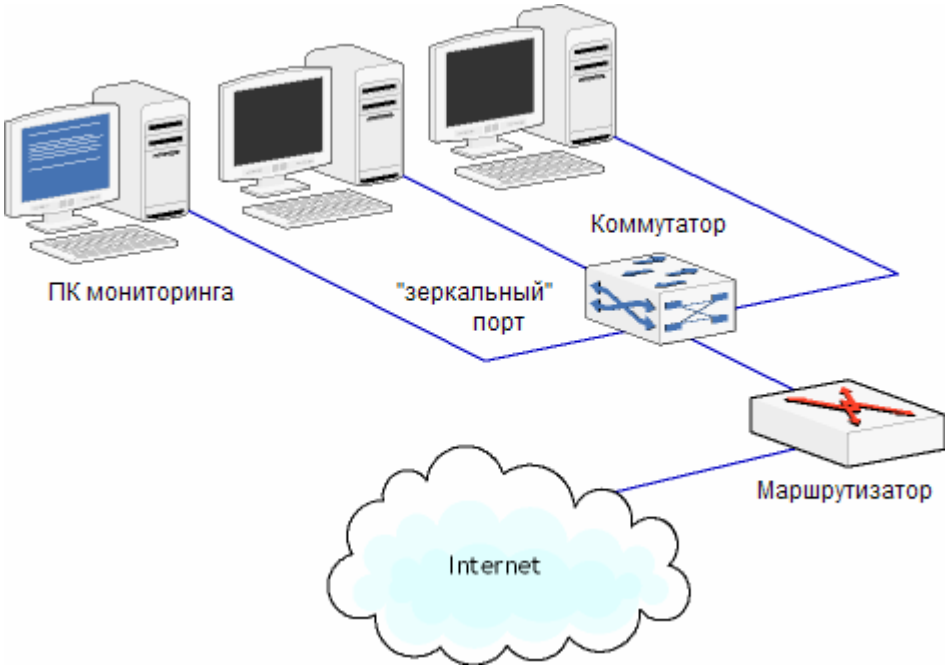
Если вам нужны подробные инструкции по изготовлению подобных кабелей, то вы легко их найдете в Интернете.

Мониторинг с помощью коммутаторов

Управляемый (managed) коммутатор с поддержкой зеркалирования (mirroring) портов (функция, позволяющая перенаправлять трафик с одних портов на определенный порт коммутатора) – идеальное устройство для сетевого мониторинга. Настройки зеркалирования портов зависят от модели и производителя (существуют десятки подобных моделей, с ценами от $100 до нескольких тысяч).

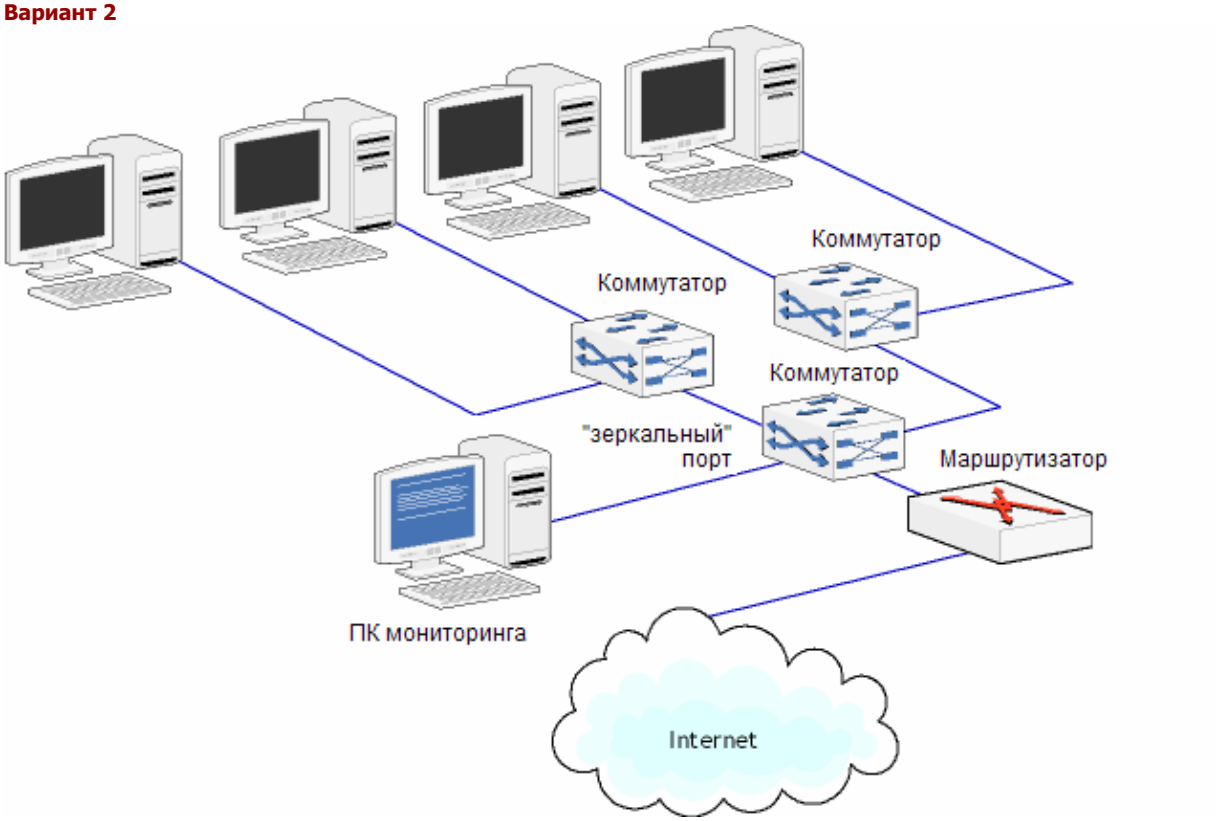
Ниже показаны два типичных варианта с использованием зеркалирования портов.

Вариант 1



В этом варианте главный коммутатор имеет функцию зеркалирования портов. ПК мониторинга подключен к "зеркальному" порту, на который переправляется весь трафик с локальных рабочих станций и маршрутизатора. Коммутатор можно настроить на перенаправление данных с одного или с нескольких портов.

Вариант 2



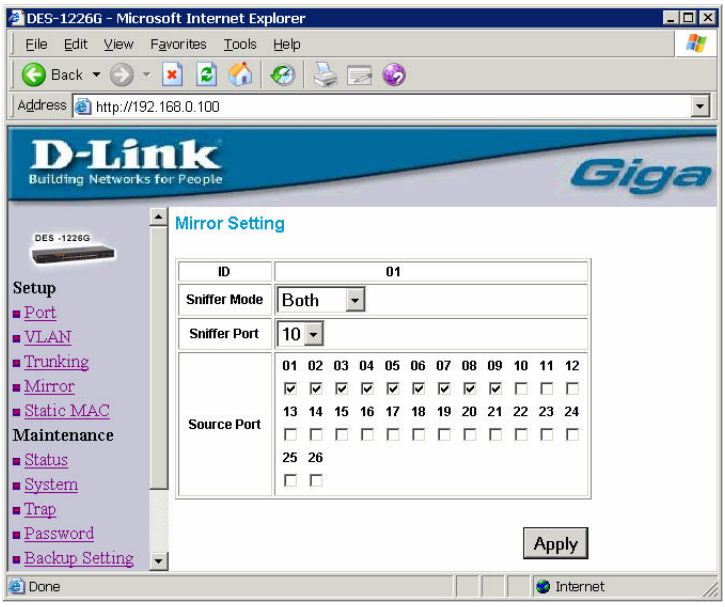
Если в сегменте вашей локальной сети используются неуправляемые (unmanaged) коммутаторы, не поддерживающие зеркалирование портов, то вы можете добавить управляемый коммутатор. Направляя Интернет-трафик через коммутатор, поддерживающий зеркалирование портов, вы подключаете ПК мониторинга к зеркальному порту и тем самым получаете возможность перехватывать трафик между локальными рабочими станциями и маршрутизатором.

Имейте в виду, однако, что при данном сетевом подключении у вас не будет возможности наблюдать трафик между локальными рабочими станциями, поскольку он проходит через неуправляемые коммутаторы, и, следовательно, не доходит до управляемые коммутатора.

Заметим, что некоторые коммутаторы, не поддерживающие зерклирование портов, все-таки могут быть использованы для мониторинга в режиме “promiscuous”. В результате некоторых видов сетевых атак, например, “ARP Flood” или “ARP Spoofing”, коммутатор начинает рассылать пакеты по всем портам. Но такие способы мониторинга не рекомендуются.

Настройка зеркалирования порта

Как мы уже упоминали, на рынке в данный момент существует множество коммутаторов с поддержкой функции зеркалирования. Всегда помните, что производители сетевого оборудования могут использовать различные названия одной и той же функции. Она может называться called "Port mirroring", "Switched PortAnalyzer" (SPAN) или "Roving analysis port" (RAP). Для настройки зеркалирования обратитесь к документации вашего коммутатора. Как правило, процесс настройки быстр и прост. Ниже представлена иллюстрация, показывающая настройку функции зеркалирования для простого и доступного коммутатора DES-1226G фирмы D-Link.



Перейдя в пункт меню **Mirror** веб-консоли управления, выберите опцию **Sniffer Mode** (Tx, Rx или Both), затем **Sniffer Port**, т. е. порт, на который будут переправляться пакеты, а также **Source Ports**, откуда будут перехватываться пакеты для их переправки в Sniffer Port.

Рекомендации по применению

Все вышеперечисленные конфигурации сетей могут быть использованы для мониторинга, но не все одинаково хороши в плане производительности и безопасности. Мы хотели бы дать следующие рекомендации по выбору конфигурации сети:

- Используйте выделенный компьютер для мониторинга. Мониторинг загруженной сети – это задача, создающая большую нагрузку на процессор, и ее не рекомендуется выполнять на компьютере, где выполняются другие подобные задачи. Особенно это касается сервера приложений, например, Web- или Ftp-сервера, поскольку мониторинг сильно снизит их производительность. Выбирайте компьютер с быстрым процессором и по крайней мере с 512 Мб оперативной памяти.

- Где возможно, используйте управляемые коммутаторы, а не хабы. Коммутаторы дают лучшую производительность и переправляют пакеты только в один порт, тем самым снижая риск несанкционированного мониторинга.

Удаленный мониторинг

Существуют ситуации, когда мониторинг вне собственного сегмента сети бывает очень полезен. Например, программисту требуется выявить проблемы в работе сетевого ПО в другом здании или даже на другом конце земного шара. В таком случае возможность наблюдать пакеты, проходящие через удаленный компьютер, может оказаться чрезвычайно ценной. Данную задачу можно решить двумя способами.

Первый способ достаточно прост и очевиден: в связи с широким распространением программ удаленного доступа, включая доступные в последних версиях инструменты Microsoft Remote Desktop Connection и Terminal Services, любой пользователь может установить на удаленной системе сетевой анализатор и получить к нему доступ через удаленный рабочий стол (Remote Desktop).

Второй способ основан на использовании удаленных сетевых агентов, т. е. программ, установленных на удаленной системе. Подключившись к одному или к нескольким удаленным агентам из одного центра, администратор видит в своей программе мониторинга весь трафик с удаленных машин в режиме реального времени. Такой подход дает ряд преимуществ, например, одновременное подключение сразу ко многим удаленным модулям и возможность анализировать/сохранять данные на вашем компьютере. Но в этом случае потребуется хороший канал связи между модулем и анализатором, а также грамотная настройка фильтров.

Хорошим примером технологии удаленного мониторинга может служить CommView Remote Agent; это первый подобный продукт на рынке и он до сих пор остается лидером в данной области. Помимо обычных преимуществ технологии удаленного мониторинга, этот продукт предлагает сжатие и надежное шифрование данных.

Сети Wi-Fi (802.11)

Вокруг promiscuous-мониторинга WiFi-сетей часто возникает много путаницы, особенно среди пользователей, которые профессионально не занимаются разработкой ПО для беспроводных сетей. Может показаться логичным, что если любой Ethernet-адаптер годится для мониторинга локальных сетей, то и любой беспроводной адаптер годится для тех же целей в сетях 802.11 a, b или g. Теоретически это верно, но на самом деле это далеко от реального положения дел.

Ситуация такова, что стандартные драйверы для беспроводных карт не поддерживают promiscuous-мониторинг (или, как еще называют эту функцию, "RF-мониторинг"). Несмотря на то, что адаптер может принимать радиосигналы определенной частоты независимо от MAC-адреса назначения, содержащегося в пакете, драйвер игнорирует все пакеты, не адресованные данному адаптеру. И нет никаких способов заставить стандартный драйвер передавать эти пакеты в программу сетевого мониторинга.

Некоторые производители программ сетевого мониторинга предлагают решение данной проблемы с помощью специальных драйверов с возможностью RF-мониторинга для ограниченного количества беспроводных карт. Таким образом, достаточно иметь поддерживаемую беспроводную карту, заменить исходный драйвер специальным – и вы можете осуществлять мониторинг беспроводной сети. Часто возникает вопрос – "Поддерживает ли моя карта режим promiscuous"? К сожалению, данный вопрос лишен смысла. Это зависит от наличия драйвера. Правильный вопрос должен звучать так: "Существует ли драйвер RF-мониторинга для моей Wi-Fi-карты и операционной системы?".

Когда ваш сетевой анализатор запущен и работает, вам необходимо оставаться в пределах действия сигнала. Пожалуй, это единственное условие мониторинга. Программа перехватит и отобразит пакеты беспроводной сети, покажет узлы и точки доступа, уровень сигнала и другие важные показатели и статистику.

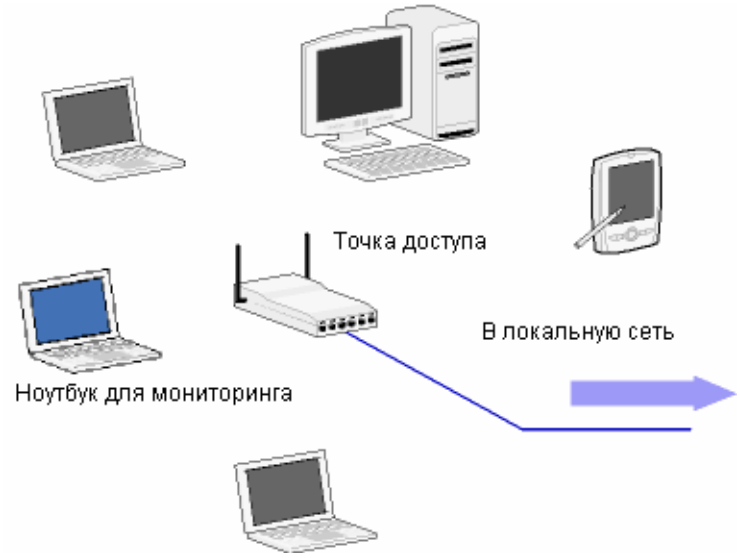
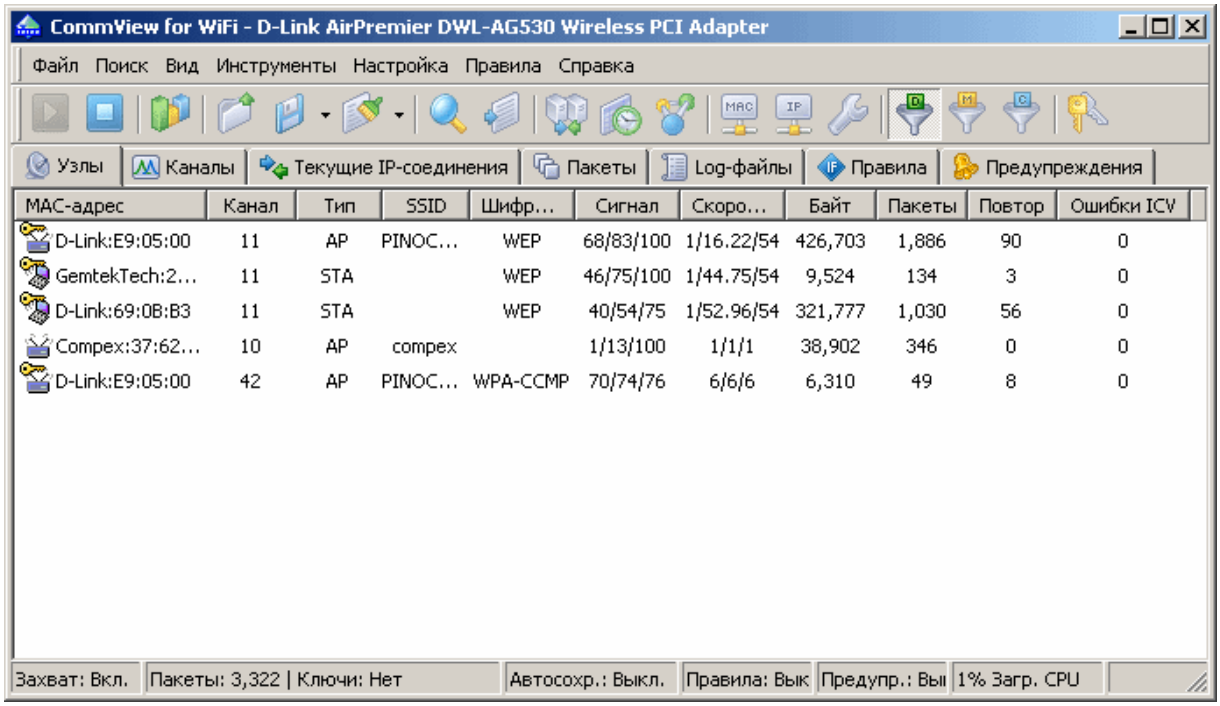
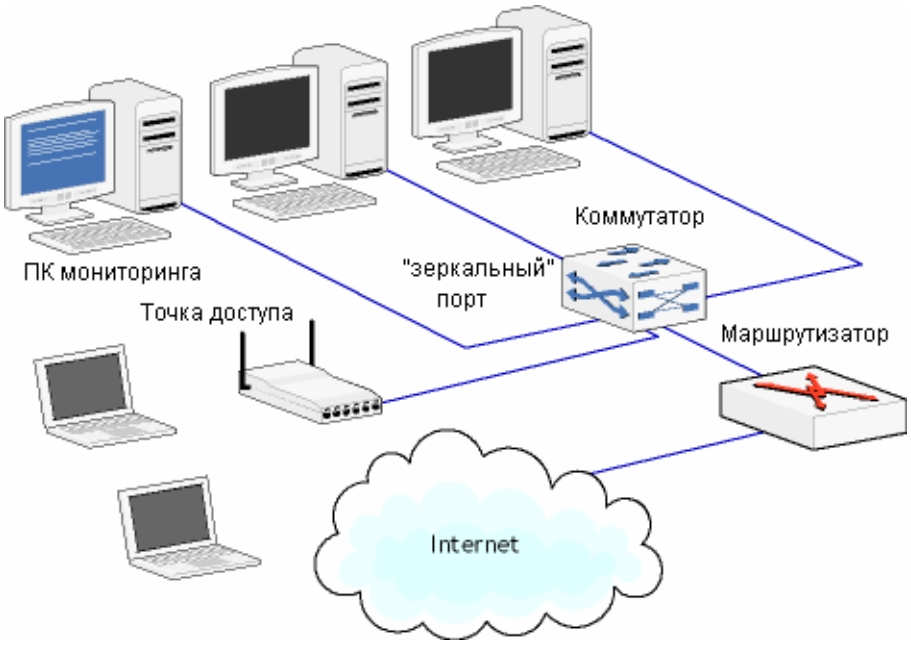


Схема беспроводного мониторинга достаточно проста: несколько компьютеров и точек доступа, а также компьютер с сетевым анализатором поблизости. Ваш сетевой анализатор покажет узлы беспроводной сети примерно следующим образом:



Помимо проблем с драйверами сетевых карт, трафик в беспроводной сети иногда зашифрован с помощью WEP (более старый метод) или WPA. Хороший сетевой анализатор должен быть способен расшифровать зашифрованный трафик "на лету" с помощью введенного пользователем ключа WEP или WPA-PSK.

Если вам всего лишь нужно наблюдать трафик между беспроводными станциями и Интернетом, то можно обойтись без сетевого анализатора для беспроводных сетей. Для перехвата входящего и исходящего трафика точки доступа достаточно стандартного мониторинга зеркального порта. Конфигурация сети для данного метода мониторинга показана ниже.



Стоит отметить, что в рамках данной конфигурации вы не сможете наблюдать трафик между беспроводными станциями и получать доступ к таким характеристикам беспроводной сети, как уровень сигнала, скорость передачи данных или узнавать о попытках вторжения.

Заключение

Существует неограниченное количество конфигураций сети. Тем не менее, понимание основных принципов сетевого мониторинга позволит пользователю обеспечить прозрачность сети практически в любой ситуации. Естественно, прозрачность сети не является конечной целью. Это всего лишь основа, требующаяся для правильной и грамотной работы с программами сетевого анализа и мониторинга.

Компания TamoSoft предлагает целый спектр современных решений для сетевого мониторинга для администраторов проводных и беспроводных сетей, профессионалов в области сетевой безопасности, судебных экспертов и разработчиков программного обеспечения. Ознакомительные версии программ всегда доступны на нашем сайте.

О компании TamoSoft

Компания TamoSoft разрабатывает передовые программные продукты, связанные с безопасностью и мониторингом Интернета и локальных сетей. В соответствии с современными требованиями, мы предлагаем профессиональные инструменты, поддерживающие самые современные стандарты, протоколы, программное обеспечение и устройства как для проводных, так и для беспроводных сетей.

Имея среди своих клиентов такие компании, как Motorola, Siemens, Ericsson, Nokia, Cisco, Lucent Technologies, Nortel Networks, Unisys, UBS, Olympus и General Electric, TamoSoft является одной из самых быстрорастущих фирм на рынке производства программного обеспечения. Продукты компании доступны как через веб-сайт, так и через сеть дистрибьюторов.

Основанная в 1998 году как подразделение по разработке программного обеспечения кипрской консалтинговой компании, в настоящее время TamoSoft - частная компания со штаб-квартирой в городе Christchurch, Новая Зеландия. В компании работает многонациональная команда, создавая надежное программное обеспечение для пользователей более чем из 100 стран, а сама компания поддерживает партнерские отношения с лидерами сферы сетевых технологий и сервиса, например, Zone Labs, Visualware и CWNP.

TamoSoft
PO Box 1385
Christchurch 8015
New Zealand
www.tamos.ru